STATEMENT OF
ANDREW M. GEISSE
CHIEF INFORMATION OFFICER
SBC SERVICES, INC.

BEFORE THE
COMMITTEE ON SCIENCE
UNITED STATES HOUSE OF REPRESENTATIVES
ON
CYBERSECURITY: U.S. VULNERABILITY & PREPAREDNESS

September 15, 2005

Thank you, Chairman Boehlert, Ranking Member Gordon and Members of the Committee.

I am pleased to represent SBC Communications on this panel focused on cybersecurity within our nation's critical industries.

SBC has a long history of providing reliable communication services. SBC provides voice and data communications services as a local exchange carrier within thirteen states and nationally with long distance, data and internet services. We also have a national wireless presence in Cingular Wireless in a partnership with BellSouth. We recognize the importance of our nation's critical communication infrastructure and the role it plays for the protection of the United States and its citizens. Integrity and reliability of our networks have been historic cornerstones of the communications industry.

As society becomes more and more dependant on information technology, cybersecurity must be a priority to protect the services provided by those same resources.

How does the communications sector depend on public and private information systems?
SBC well understands the strong connection between communications security and information technology, or what is commonly referred to as cybersecurity.

Behind the networks that move voice and data, are many applications, private networks, and computing resources. These resources support the operations, administration, maintenance, and provisioning services of our telecommunications infrastructure. These information systems and networks provide SBC and other carriers the ability to manage this complex industry supporting the dial tone and Internet connections that we have all come to expect as a part of our daily lives. Securing these cyber resources to ensure the integrity and availability of communications networks is a role that SBC takes seriously, as part of its corporate culture.

SBC uses many vendor products within its information technology infrastructure. In that regard, SBC is dependent on vendor product development in the private sector and

delivery of private sector services and materials to support the information technology services of the infrastructure. In this manner, SBC relies on vendors to incorporate cybersecurity best practices, standard interfaces, and administrative tools within their products. SBC is also reliant on vendors to ensure their software products can be patched easily to prevent existence of long term vulnerabilities.

In support of the private sector, SBC provides managed security services as a product offering. These types of services include: risk reviews and analysis, firewall installation and monitoring, and firewall and intrusion prevention / detection reseller for other vendor products.

For the consumer space, SBC's Internet Services organization through our relationship with Yahoo! provides security tools to our Internet Services customers as part of their Internet experience. In this manner, SBC supports cybersecurity to the consumer so they can better protect their home information technologies, which in turn provides less problems to the shared Internet space.

Other areas where SBC has focused on consumer cybersecurity is as a founding member of the Internet NOC Hotline, which connects key US and International ISPs. SBC is also a founding member of the Global Infrastructure Alliance for Internet Security.

An area where SBC would recommend government focus is on the education of the consumers regarding cybersecurity matters. End users must recognize they are part of the interconnected world. When end-users do not understand how virus and worm propagation can impact their home PC's, the result is a negative effect at the Internet level. This impact is caused through a variety of malicious activities, including, SPAM e-mails and bot-networks. Educational awareness programs should advise users on anti-virus protection and identity theft protection.

What steps is SBC taking to secure its systems?
At SBC, we implement physical and cybersecurity measures that protect both our customer-serving network facilities and our internal information services. Physical security measures include guard services, card key technologies, visible badge policies, video monitoring, and, in special cases, bio-metric technologies.

Information security begins with a cybersecurity policy that is part of our Corporate Code of Business Conduct. We segment our internal network connections from external networks using various security technologies to ensure the integrity of our network. We keep our internal core business networks separate from the general employee network. Virus protection software is deployed as standard on desktops and e-mail servers. Pro-active vulnerability scanning is performed constantly to identify potential areas of risk.

SBC maintains close ties to government agencies responsible for national security. We work closely with them on a daily basis to receive and share security related information. Examples are the National Security Telecommunications Advisory Council (NSTAC),

National Coordinating Center Telecom Information Sharing and Analysis Center (NCC Telecom ISAC), Infragard, and the National Security Information Exchange (NSIE).

Internally, SBC has several organizations dedicated to the security of our assets. Organizations such as our National Security / Emergency Preparedness organization, our Asset Protection organization, and our Corporate Information Security organization, work to protect our customers information and services, our employees, and our internal networks and data on a daily basis.

Our SBC Labs business unit works closely with technology vendors, academic communities, and government standards organizations, to partner and share information on new technologies. Cybersecurity standards are always a priority in future service and technology development and a focus of our internal auditing organization as well as external security audits.

Continued Government focus on security standards and collaborative support organizations is seen positively by SBC. Providing research assistance, grants, and funds to focus the information technology industry to work towards security standards and best practices is necessary. It is important that the Government provides to the critical infrastructure industries the learnings and best practices that its cybersecurity agencies learn.

Legislation should not always be necessary to bring industry attention to technical priorities. However, providing research assistance, grants, and funds to focus the information technology industry to work towards security standards and best practices is necessary.

What are the possible consequences for the communication sector of disruption or attack on information systems?

Society in the 21st century is rapidly changing with increasing reliance on information technologies. Users' expectations are that they be mobile and have instant access to the Internet and their e-mail. Providing secure services in this environment becomes increasingly important and challenging. Federal programs could help educate and assist consumers to understand their roles and responsibilities in a connected world.

To illustrate: Consider how often people stop for gas and use a payment card at the pumps for convenience. The payment card transactions must be carried efficiently, reliably, and securely across communications networks. This is to ensure the gas vendor, the payment card vendor, and the customer are all satisfied that the transaction occurred to everyone's expectation.

The networks, the applications, and the information systems that are necessary to complete transactions of this nature are part of our society on a daily basis. Cybersecurity is necessary to ensure the integrity of those transactions. Disruptions within the communications sector can impact these, and other, daily activities.

Consider the impact of disrupted or unreliable communications to everyday needs, including how patients obtain collaborative health care between multiple providers and locations. Communications plays ever increasing importance to health industries, emergency first responders, 911 services, law enforcement, banking, power, and other parts of our society that serve critical functions.

With the growing use of wireless technologies, we must recognize that those wireless systems still rely on an underlying physical transport, use of back-end systems and applications that may interconnect with other carriers. As we have recently witnessed in New Orleans and the Gulf Coast, if the supporting infrastructure is disrupted, communication fails. A cyber disruption could cause similar impacts as a physical disruption.

While we recognize that other critical infrastructure industries are reliant on the communications industry to provide the network and communication services, we also recognize that we, as an industry, are reliant on those other industries. We require industries such as electricity and gas, banking and finance, health, and government, to also function securely and without disruption to ensure the integrity of our communications infrastructure.

As recognized by the Department of Homeland Security, the nation is dependent on the critical infrastructure of communications, banking and finance, power, food, health, information technology and others. A disruption to any component affects the whole infrastructure. Securing against disruptions to any component is in the best interest of all.

In what areas are current cybersecurity technical solutions for the communications sector inadequate?
Where is further research needed to mitigate existing and emerging threats and vulnerabilities?

The communications industry is also increasingly dependent on application and information technology vendors to ensure the products they provide are of the highest quality and integrity. Software and hardware that does not meet industry security best practices and standards require additional efforts and expense to meet its expected function. Vendors that provide software or hardware with security vulnerabilities that must constantly be monitored, reviewed, and patched, are a drain on a company's resources and a liability to companies that must ensure the integrity of their systems, data, and services.

SBC works diligently with software vendors that provide the foundation of the information technology infrastructure to ensure necessary software security patches are installed to protect our complex environment. Continued focus from the Federal Government on industry standards for secure information technology products is appreciated and desired. This will help to ensure that better security and quality is an objective of the software, network and computer hardware industries.

NIST (National Institute for Standards) is one example of a collaborative organization that has been helpful in promoting information security requirements through its various research and standards efforts. We, as a business, look to leverage those standards as potential baselines in our efforts and are glad to see vendors meet such useful guidelines.

How should federal agencies, such as DHS, the National Science Foundation, the National Institute of Standards and Technology, and the Defense Advanced Research Projects Agency, and the academic researchers work with industry to define priorities for and support research in these areas?

Cybersecurity must become a priority in the creation of new information technologies. To date, security components for information technologies often appeared to be an afterthought. Examples of this can be seen in early versions of cellular and Wi-Fi technologies, where calls could be intercepted, cell phones cloned, and data snooping could occur.

Internet Protocol (IP) based services wrestle constantly with the need to traverse the same network paths where unscrupulous persons may have the ability to interfere, impede, or intrude on the service itself. IP based services must find new ways to protect the content of each packet that is carried and delivered in this shared Internet world.

We have all seen that virus and worm attacks have risen over the past several years. Research focus on how to prevent the distribution of malicious content through virus, worms, and e-mail should be a high priority for all industries that use the Internet for communications and business. The ability to detect and remove unwanted data content and attacks as it progresses through the network is more desirable than expecting each end device to have the same ability to protect itself from its neighbors on the networks.

Admittedly, security requirements interfere with convenience of the product or service offered. However, we need cybersecurity and software development standards that insist new technologies embrace security as part of their evolution and development. In this way, society as a whole benefits through improved assurance of integrity, reliability, service, and subsequent reduced resource costs to support those services.

SBC is committed to work with the information industry to build the next generation of Internet-based voice, video and data communications, securely.

What are the most critical responsibilities of the Department of Homeland Security (DHS) in cybersecurity for the communications sector and what are the most urgent steps the new Assistant Secretary for Cybersecurity and Telecommunications should take?

Mr. Chairman and members of the committee, your assistance to focus industry attention on cybersecurity is greatly appreciated. We encourage the Department of Homeland Security to continue:

- to support research grants and assistance that focus on National cybersecurity,
- to support industry organizations and government agencies that create security standards and best practices.

- to continue to provide early warnings of security events, through various government agencies
- and to make sure the security best practices that various critical government agencies develop are shared with our critical infrastructure industries.

I would like to add that you should make sure our laws carry serious penalties for cybersecurity issues and that the instigators are prosecuted to the full extent of the law. It must become a major crime. It is no longer just kids playing with computers. The attacks are serious.

Thank you for the opportunity to appear before you today. The work you are doing is critical to our future as a nation. Cyber terrorism is a real threat and we must stay diligent.